UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/730,681	12/08/2003	Joon-Kit Goh	SE0039	5707

29393 7590 10/06/2008

ESCHWEILER & ASSOCIATES, LLC
NATIONAL CITY BANK BUILDING
629 EUCLID AVE., SUITE 1000
CLEVELAND, OH 44114

EXAMINER	
PATEL, NIRAV B	
ART UNIT	**PAPER NUMBER**
2135	

NOTIFICATION DATE	DELIVERY MODE
10/06/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing@eschweilerlaw.com

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 10/730,681	**Applicant(s)** GOH, JOON-KIT	
	Examiner NIRAV PATEL	**Art Unit** 2135	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 15 September 2008 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: *None*.
   Claim(s) objected to: *None*.
   Claim(s) rejected: *1 and 3-26*.
   Claim(s) withdrawn from consideration: *None*.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☐ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: _____.
12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

/KimYen Vu/
Supervisory Patent Examiner, Art Unit 2135

Continuation of 11. does NOT place the application in condition for allowance because: Applicant's arguments, regarding to claim rejections, filed Sep. 15, 2008 have been fully considered by they are not persuasive.

Regarding to applicant argument to Examiner's response on July 18, 2008, Examiner disagrees and maintains since, Qi's invention relates to implementing a cryptography engine to perform cryptography algorithm such as a DES algorithm. The cryptography engine for performing cryptographic operations (such as DES, Triple DES - 3DES) on a data block is provided. The cryptography engine includes a key scheduler configured to provide keys for cryptographic operations. As shown in Fig. 4a, the DES engine, includes input FIFO to decouple the DES engine from surrounding logic. A 64-bit data block is combined with an initialization vector from initialization vector block. The 64-bit block then undergoes an initial permutation, before round 1. Two-level multiplexer stage contains four multiplexers for determining whether to load initial data, swap data from the previous round, or not swap data from the previous round. Initial data is loaded in the first round of DES processing. Data is swapped between rounds of DES processing. Data is not swapped in triple DES between the completed 16 rounds of DES processing. Control logic can track the round number in order to determine what signals to send to the multiplexers. According to various embodiments eight Sboxes are provided in Sbox stage 427.The 32-bit output of Sbox stage is provided to permutation stage 429. A permutation stage 429 maps input bits in certain positions to different output positions. The 32-bit output of permutation stage 429 is combined with an XOR with the value in register 411 at 431. The result of the XOR is provided to the register 411 through multiplexer stage 409 for the next round of DES processing. That is, the right half is expanded, combined with an XOR function with a version of the key, provided to a Sbox stage, permuted, and combined with an XOR with the left half. After the last round, the outputs are written to register 433 and register 435. The output can then undergo a final permutation at 437. The result of a final permutation at 437 is combined by way of an XOR with an initialization vector as noted above when the DES engine is used to decrypt data. Otherwise, the result of the final permutation at 437 can remain unchanged by combining by way of an XOR with a sequence of zeros. For triple DES, the outputs at 433 and 435 are passed back to multiplexer stage 409. Control circuitry determines how to pass the data back to register 411 and 413 for a next 16 rounds of DES processing. In this case, Qi teaches the DES engine/cryptography engine for performing 3DES operation. Further, in an analogous art, Anand's relates to the field of cryptography, in particular to block ciphering and to implementations of the triple data encryption algorithm for the data encryption standard. The portion 200 is preferably implemented with either one, three, four, eight or sixteen cipher round blocks, each performing their cipher round operations preferably during one clock cycle. Since DES ciphering requires sixteen rounds of ciphering, one clock cycle is needed if sixteen cipher round blocks are implemented, two clock cycles are needed when eight cipher round blocks are implemented, four clock cycles are needed when four cipher round blocks are implemented, and six clock cycles are needed when three cipher round blocks are used. The cipher block portion 200 reduces the number of XOR operations in the critical timing path. The permuting function (Ef) operates on both the left input as well as the output from the permuting function (Pf). The output of left permuting function (Ef) (220) is XOR'ed (222) with the key producing an output which is stable in time much earlier than the S-box output. The critical timing path for each round of ciphering thus comprises the path through the S-box, the permuting function (Pf) and XOR gate (224), which is one less XOR gate that standard DES implementations. In this case, Anand discloses the improved cryptography engine for performing the DES operation by reducing time required for critical path operation. Therefore, the prior art is replete with references disclosing DES engine for performing 3DES operation that provide the improved cryptographic DES operation by reducing the timing requirement for critical path operation. A recitation directed to the manner in which a claimed apparatus is intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)). Since, applicant has failed to pointed out how the specific result performed by the claimed DES engine is different from the prior art, it is believed that the rejections should be sustained.